RECORD
AND
BRIEFS

No. 16-402

IN THE

Supreme Court of the United States

TIMOTHY IVORY CARPENTER,

Petitioner,

—v.—

UNITED STATES OF AMERICA,

Respondent.

ON WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT

REPLY BRIEF FOR PETITIONER

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, DC 20005

Cecillia D. Wang
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

TABLE OF CONTENTS

TABLE OF AUTHORITIES ii

REPLY BRIEF FOR PETITIONER 1

I. LAW ENFORCEMENT'S ACQUISITION OF LONGER-TERM HISTORICAL CSLI IS A SEARCH 2

A. People Have A Reasonable Expectation Of Privacy In Longer-Term Historical CSLI. 2

B. Procuring CSLI Intrudes on People's "Papers" Under the Fourth Amendment 14

C. The Government's Theory Would Negate Fourth Amendment Protection For A Wide Range Of Vital Privacy Interests In The Digital Age 16

II. WARRANTLESS SEARCH OF LONGER-TERM HISTORICAL CSLI IS UNREASONABLE UNDER THE FOURTH AMENDMENT 18

A. The Subpoena Power Does Not Allow The Government To Obtain Records Held By A Third Party In Which There Is A Reasonable Expectation Of Privacy 18

B. Principles Of Fourth Amendment Reasonableness Require A Warrant... 22

C. Congressional Inaction Is Irrelevant Here 24

CONCLUSION 25

TABLE OF AUTHORITIES

CASES

Alderman v. United States, 394 U.S. 165 (1969) 22

Couch v. United States, 409 U.S. 332 (1973) 19, 21

Dickman v. C.I.R., 465 U.S. 330 (1984) 15

Donovan v. Lone Steer, Inc., 464 U.S. 408 (1984) 19

Ex Parte Jackson, 96 U.S. 727 (1877) 16

Fisher v. United States, 425 U.S. 391 (1976) 19, 20

Ford v. State,
477 S.W.3d 321 (Tex. Crim. App. 2015) 24

Hoffa v. United States, 385 U.S. 293 (1972) 11

Kyllo v. United States, 533 U.S. 27 (2001) 2, 3, 5

Lebron v. Nat'l R.R. Passenger Corp.,
513 U.S. 374 (1995) 14

Maryland v. King, 133 S. Ct. 1958 (2013) 22

Minnesota v. Olson, 495 U.S. 91 (1990) 11

Pension Ben. Guar. Corp. v. LTV Corp.,
496 U.S. 633 (1990) 24

Riley v. California, 134 S. Ct. 2473 (2014) .....*passim*

See v. City of Seattle, 387 U.S. 541 (1967) 21

Shades Ridge Holding Co. v. CIR,
23 T.C.M. (CCH) 1665 (1964) 13

Smith v. Maryland, 442 U.S. 735 (1979) 2, 7, 8, 9

State v. Ford, 454 S.W.3d 407 (Mo. Ct. App. 2015) ... 6

State v. Roberts,
No. 13-009778CF10A (Fla. 17th Cir. Ct. May 3, 2016) 6

United States v. Brown,
2017 WL 4216979 (D. Neb. 2017) 23

United States v. Gaskins,
690 F.3d 569 (D.C. Cir. 2012) 13

United States v. Gramlich,
551 F.2d 1359 (5th Cir. 1977) 13

United States v. Jacobsen, 466 U.S. 109 (1984). 11, 12

United States v. Johnson,
480 F. App'x 835 (6th Cir. 2012) 13

United States v. Jones, 565 U.S. 400 (2012) .....*passim*

United States v. Karo, 468 U.S. 705 (1984) 5

United States v. Miller, 425 U.S. 435 (1976) ....*passim*

United States v. Warshak,
631 F.3d 266 (6th Cir. 2010) 20

United States v. Williams,
504 U.S. 36 (1992) 14

Young v. Owens, 577 F. App'x 410 (6th Cir. 2014) .. 13

U.S. CONSTITUTION & STATUTES

U.S. Const. amend. IV .....*passim*

18 U.S.C. § 2702(a)(3) 12

18 U.S.C. § 2702(c)(4) 12

18 U.S.C. § 2703(d) 22, 23, 24

47 U.S.C. § 222 ..... 9, 10

47 U.S.C. § 222(c)(1) 10

47 U.S.C. § 222(c)(3) 10
47 U.S.C. § 222(d)(4) 10
47 U.S.C. § 222(f) 10

RULES

Fed. R. Evid. 803(6) 15

LEGISLATIVE MATERIALS

Email Privacy Act, H.R. 699, 114th Cong. (2015) ... 24

OTHER AUTHORITIES

Google Terms of Service,
https://www.google.com/policies/terms 17

Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* (2015) 7

REPLY BRIEF FOR PETITIONER

Cell phones (and related mobile devices) are increasingly indispensable tools of modern life. It is essential that people not only own such devices but also that they carry them virtually all the time, wherever they go. As the Technology Companies explain, it is an inescapable fact that such devices reveal locational information to service providers "by dint of their mere operation." Tech. Cos. Br. 11.

The government argues that the consequence of this technological landscape is that Americans no longer have any right to privacy in the aggregation of their movements over time. Simply by using cell phones, the government maintains, the populace gives law enforcement constitutionally unchecked authority to collect a detailed record of every person's historical whereabouts—without probable cause, a warrant, or any Fourth Amendment protection whatsoever.

This cannot be right. The American people have a reasonable expectation that the details of their minute-by-minute travel over time remain private, as they always have been. A proper understanding of the Fourth Amendment renders law enforcement's procurement of longer-term CSLI a "search." And the only way such a search can be reasonable is with a warrant.

I. LAW ENFORCEMENT'S ACQUISITION OF LONGER-TERM HISTORICAL CSLI IS A SEARCH.

A. People Have A Reasonable Expectation Of Privacy In Longer-Term Historical CSLI.

Citing principally to *Smith v. Maryland*, 442 U.S. 735 (1979), and *United States v. Miller*, 425 U.S. 435 (1976), the government urges the Court to ignore the sea change in technology that made possible the search of 127 days of petitioner's location data, and to decide this case through wooden application of legal principles from a bygone era. *See* Resp. Br. 32-33. But this Court's more recent precedent dictates that the government cannot capitalize on new technology to shrink privacy. And even on their own terms, *Smith* and *Miller* do not control here.

1. In the face of technological change, the Fourth Amendment "assures preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted." *Kyllo v. United States*, 533 U.S. 27, 34 (2001); *see also Riley v. California*, 134 S. Ct. 2473, 2495 (2014) (warrant requirement applies to cell phones seized incident to arrest to safeguard "the privacies of life" previously protected by that requirement). Five concurring Justices applied that principle in *United States v. Jones* to hold that GPS tracking constitutes a search because people never expected before the advent of modern location-tracking technology that compilations of their movements for weeks on end would be readily accessible to government agents. 565 U.S. 400, 429-31 (2012) (Alito, J., concurring in the judgment).

As with the GPS technology in *Jones*, the advent of cellular service technology has given the government access to locational information previously unimaginable, and has so lowered the cost of obtaining this information as to remove all practical impediments to massive incursions on privacy. *See* Tech. Experts Br. 22-25; Elec. Frontier Found. Br. 16 n.32. People have always had a reasonable expectation that no one other than themselves would know everywhere they have traveled for extended periods of time. No one could have decided after the fact to track another person's movements retrospectively, and to instantaneously pluck that historical record out of thin air.

That is what the government says it—and, by extension, state and local police agencies—can now do. Yet neither of its arguments for distinguishing the anti-shrinkage principle in *Jones*, *Kyllo*, and *Riley* holds up.

a. Contrary to the government's contention (Resp. Br. 33), it does not matter that *Jones* and *Kyllo* involved police officers' use of their own technology, whereas here the government is capitalizing on technology deployed by others. The means the government uses to obtain information is sometimes relevant, but so too is the nature of the information obtained. That is why the concurring Justices in *Jones* suggested that the same concerns animating their conclusion that a search took place would have been raised by "surreptitiously activating a stolen vehicle detection system" in Jones's car or conducting GPS tracking of his phone. 565 U.S. at 426, 428. Likewise, the Court in *Riley* applied the full protections of the Fourth Amendment to searches of

cell phones even though the privacy intrusion was purely a function of the storage capacity of the phones themselves; the government used nothing more than its agents' hands and eyes to conduct the searches at issue. 134 S. Ct. at 2480-81.

In a democratic society, it is vital to safeguard a sphere of individual privacy in which people can conduct their affairs free of unwarranted government intrusion. *See Riley*, 134 S. Ct. at 2494-95; *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring). Here, as in *Jones* and *Riley*, the power the government seeks would dramatically unsettle the balance between personal liberty and state power that the Fourth Amendment was intended to preserve. It does not matter whether the government seeks to use its own technology or to leverage a private industry's new technology to conduct surveillance. Either way, the chilling effect would be the same.

b. Nor can the government distinguish *Jones* on the ground that CSLI is substantially less revealing than GPS information. The government's argument based on two individual location points from petitioner's records dating back to 2010 (Resp. Br. 24-27) dramatically understates the privacy stakes at issue.

i. Even when individual points of location data place a person within a relatively large cell site sector, the aggregation of just a small number of such points can reveal significantly more precise information than one point alone. Petr. Br. 24-26. In this case, a limited analysis of petitioner's CSLI data by the American Civil Liberties Union as amicus in the court below determined when petitioner spent the night in an area consistent with his home, and

when he slept in a neighborhood four miles away, as well as his habit of traveling to the same spot in Detroit on Sunday afternoons—an area consistent with the location of his church. 6th Cir. Doc. No. 29, at 11-12. This is the same kind of information that motivated the concurring Justices in *Jones*.

ii. The government's observation that "reasonable inferences or additional evidence" may sometimes be necessary to interpret the significance of CSLI (Resp. Br. 24) makes no difference. This Court has rejected "the novel proposition that inference insulates a search." *Kyllo*, 533 U.S. at 36. The proposition is "blatantly contrary" to the Court's holding in *United States v. Karo*, 468 U.S. 705 (1984), "where the police 'inferred' from the activation of a beeper that a certain can of ether was in the home." *Kyllo*, 533 U.S. at 36.

The possibility that inference or additional evidence may be necessary to interpret location data is also true of the GPS tracking that this Court confronted in *Jones*. Tracking a car to a parking lot will not reveal whether the suspect went to the nearby jewelry store for a robbery, doctor's office for a checkup, or cafe for a meeting with a friend. Corroborating evidence is commonly required. But prolonged GPS tracking nonetheless constitutes a search. *Jones*, 565 U.S. at 429-30 (Alito, J., concurring in the judgment).

iii. The progression of CSLI technology—merging ever closer to the precision of GPS, and bound in the near future to be virtually the same—clinches the applicability of *Jones* to the situation here. Petr. Br. 26-29. The government urges this Court to ignore this progression on the grounds that

(1) "no case" has yet dealt with current technology and (2) CSLI technology "could develop in a different direction." Resp. Br. 27. Neither argument is persuasive.

Courts are *already* adjudicating cases where the government obtained precise historical cell phone location data that relies on carriers' developing ability to "measure[] the radio frequency distance between the telephone and nearby towers, and g[i]ve an estimate of the location of the telephone itself during the call." *State v. Ford*, 454 S.W.3d 407, 410-11 (Mo. Ct. App. 2015); *see also* Br. for Appellee 30 n.10, *United States v. Fulton*, 837 F.3d 281 (3d Cir. 2016) (No. 15-1513), 2015 WL 7423166 (data showed that suspect's phone was "at the very least 1000 feet away" from the scene). Courts are likewise confronting cases involving cell phones' connections to "small cells." In one recent case, a special agent with the FBI's Cellular Analysis Survey Team explained that the suspect could not have been at a particular residence at a specified time because his phone did not connect to the small cell located nearby. Dep. of David Magnuson 33-35, *State v. Roberts*, No. 13-009778CF10A (Fla. 17th Cir. Ct. May 3, 2016).

The future trajectory of the technology is also clear. As service providers roll out the next generation cellular network (5G), small cells will play an even greater role and will be deployed in significantly greater numbers, with marked effects on the precision of CSLI. *See* Tech. Experts Br. 16-17 & n.23. Femtocells, for example, have a broadcast radius of just 10 to 20 meters, meaning that CSLI is now able to place a phone in an area as much as five

times *smaller* than the oval plaza in front of the Supreme Court. *See* Joseph Hoy, *Forensic Radio Survey Techniques for Cell Site Analysis* 69 (2015) (discussing small cell broadcast coverage); *Hodge v. Talkin*, 799 F.3d 1145, 1151 (D.C. Cir. 2015) (dimensions of Court's plaza). Similarly, precise historical location estimates produced by service providers measuring the time and angle of signals arriving at their towers can be accurate to within 50 meters or less. Tech. Experts Br. 18.

2. Even on their own terms, this Court's cases involving "the third-party doctrine" do not apply here.

a. Contrary to the government's repeated claim (Resp. Br. 15-21, 28-29), the fact that a third party has access to information has never been sufficient, on its own, to divest the information of Fourth Amendment protection. Even in *Miller* and *Smith* themselves, this Court stressed the need to "examine the nature of the particular documents sought to be protected in order to determine whether there is a legitimate 'expectation of privacy' concerning their contents." *Miller*, 425 U.S. at 442; *accord Smith*, 442 U.S. at 741. Were exposure of information to a third party dispositive, those cases would have been much more easily decided. The Court need not have considered, for example, that pen registers have "limited capabilities," "disclos[ing] only the telephone numbers that have been dialed," and not "whether the call was even completed." *Smith*, 442 U.S. at 741-42.

The contrast here is dramatic. As petitioner has explained, weeks or months of CSLI can reveal extraordinarily intimate and sensitive information,

including, most significantly, one's detailed whereabouts over extended periods of time. *See supra* at 4-5; Petr. Br. 16-17. The government has never before been able to track anyone, much less everyone, in this way. And regardless of the particular details revealed in any given set of data, the mere "[a]wareness that the Government may be watching chills associational and expressive freedoms." *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring); *see also* Ctr. for Competitive Politics Br. 11-12; Elec. Privacy Info. Ctr. Br. 20 n.7; Reporters Comm. Br. 17-22.

b. Contrary to the government's claim (Resp. Br. 31), CSLI is not "voluntarily" conveyed within the meaning of *Miller* and *Smith*. Unlike a phone number entered into a phone to connect a call or a check passed into commerce to be drawn on an account, cell phone location data does not necessarily involve any voluntary act on the part of users. The data is created whenever mobile devices receive a call, text message, or data connection, requiring no activity of a user whatsoever. Moreover, the location data does not even directly relate to the functions the device performs. Unlike the phone number necessary to place the call or the negotiable instrument necessary to transfer funds, a person using a smartphone does not consciously share her geographic location with her service provider each time someone sends her an email or her phone automatically downloads an updated weather forecast.

Moreover, the many functions smartphones perform further distinguish this case from the discrete uses of landline telephones in *Smith* and

banking services in *Miller*. A smartphone is the nerve center used to organize and manage virtually every aspect of the user's personal (and often professional) life. *See Riley*, 134 S. Ct. at 2489; Tech. Cos. Br. 14-17; Data & Society Research Inst. Br.; Petr. Br. 39-42. Carrying a device so central to one's self-expression, well-being, safety, and livelihood is not "just as volitional as . . . exposing the numbers [one] dials" to a telephone service provider, Resp. Br. 32.

And while some users may be vaguely aware that their phones have to connect to cell towers, few if any are likely to know that every such connection is recorded and maintained, even when one turns off location services on one's phone. Unlike the banking and call records at issue in *Miller* and *Smith*, cellular subscribers do not receive records from their providers showing that this information has been collected. Thus, it is a fiction to claim that the information is in any meaningful sense voluntarily shared.

c. This case is also different from *Miller* and *Smith* because a federal statute (the Telecommunications Act) protects the privacy of the information here and gives further expression to the public's expectation of privacy. The government says that Section 222 of the Act similarly protected the information at issue in *Smith*, and so recognizing its relevance would require "overruling" that case. Resp. Br. 22. But the statute postdates *Smith* by 17 years, so it could not have played any role in the Court's analysis there. More important, Section 222 gives location records a level of explicit protection above

and beyond any other telecommunications data. *Compare* 47 U.S.C. § 222(c)(1), *with id.* § 222(f).

The government also argues that the particulars of Section 222 do not support any reasonable expectation of privacy and that, in any event, statutory protections are wholly irrelevant to the reasonable-expectation-of-privacy analysis. Resp. Br. 21-22. The government is wrong on both counts.

Under the Telecommunications Act, service providers may disclose cell phone location information only in limited circumstances: in aggregate, anonymized form without customer consent, 47 U.S.C. § 222(c)(3); in individually identifiable form only with the "express prior authorization" of the customer, *id.* § 222(c)(1), (f), or in an emergency, *id.* § 222(d)(4); and as otherwise "required by law," *id.* § 222(c)(1). Focusing exclusively on the last, vague provision, the government argues that the statute puts people on notice that CSLI can be lawfully obtained under the Stored Communications Act ("SCA") without a warrant. Resp. Br. 21-22, 42-43. But of course, any statutory commands must be read consistently with the Constitution. *Clark v. Martinez*, 543 U.S. 371, 381 (2005). Providing access "as required by law" only begs the question of what the Fourth Amendment requires. If, as petitioner argues, the Fourth Amendment requires a warrant, then any mechanism for warrantless access under the SCA falls away.

Moreover, the Fourth Amendment turns on "the everyday expectations of privacy that we all share" against incursions by members of the public at large. *Minnesota v. Olson*, 495 U.S. 91, 98-99

(1990). It is thus the explicit statutory protection against unconsented access to CSLI by other members of the public, rather than any special provision for law enforcement access, that reflects societal expectations of privacy. The government's reading of the provision permitting disclosure "as required by law" as carte blanche for police agencies is contrary to Congress's plain purpose and, more fundamentally, the Fourth Amendment.

d. Finally, the cases involving human eyewitnesses or informants do not govern here. *See* Resp. Br. 18, 35 (citing *Hoffa v. United States*, 385 U.S. 293 (1972), and *United States v. Jacobsen*, 466 U.S. 109 (1984)). It is a basic truth of human interactions that a person may, upon learning information, choose to share the contents of her mind with others. Hence, this Court has long held that a person assumes the risk that a confidant may divulge such information to others, including the authorities. *Hoffa*, 385 U.S. at 303. Here, by contrast, societal expectations and a federal statute prohibit service providers from sharing CSLI with the general public.

Jacobsen is similarly inapposite. There, employees of a private freight carrier observed an apparently illicit substance in a package and, without any government involvement, chose to inform the government of what they had seen. 466 U.S. at 111. The government then inspected the package, observing the incriminating information that had already been revealed through the private company's inspection. *Id.* Here, in contrast, no employee of MetroPCS or Sprint ever had reason to view petitioner's location records. The data was kept

in an automated system for billing and network diagnostic purposes, sight unseen. Only as a result of *law enforcement* action did the companies extract petitioner's data and provide it to the government, where it was for the first time examined.[1]

3. The government's complaint (Resp. Br. 30) that it would be "unworkable" in practice to hold that the third-party doctrine does not apply here is unpersuasive. A reasonable-expectation-of-privacy analysis must be grounded in "practical" realities. *Jones*, 565 U.S. at 963 (Alito, J., concurring in the judgment). Before the advent of CSLI and GPS technology, law enforcement could rarely, if ever, track a person's historical movements on a minute-by-minute basis for a period of time covering more than a few hours. *See* Petr. Br. 18-19, 31. Thus, if the government insists on specifying "how much is too much" when it comes to CSLI, a bright-line rule allowing law enforcement agents to request no more than 24 hours of an individual's historical CSLI without triggering the warrant requirement would give the government every benefit of the doubt in practical terms and the certainty it claims to need.

At the same time, it would be sufficient to resolve this case to hold that the one week's worth of CSLI the government requested from Sprint crosses the line, wherever exactly that line may be. Even if the Sprint order should be analyzed apart from the

---

[1] *Jacobsen* is especially irrelevant because, even if employees of the service providers *had* inspected petitioner's records and seen incriminating information, they would have been prohibited by statute from voluntarily "divulg[ing it] . . . to any governmental entity" absent an emergency. 18 U.S.C. § 2702(a)(3), (c)(4).

government's overall 152-day request, that order still allowed the government to obtain seven days of CSLI. Contrary to the government's contention (Resp. Br. 56-57), there is no practical or empirical basis for believing the government would typically have secured that amount of locational information before the advent of CSLI. And while the government cites a handful of cases recounting law enforcement surveillance, it offers no reason to believe they are anything other than outliers.

Moreover, only one of the cases the government cites actually involved anything close to longer-term, round-the-clock surveillance (although even there, it is impossible to tell from the opinion in the case the extent to which the suspect was continuously tailed). *United States v. Gramlich*, 551 F.2d 1359 (5th Cir. 1977). A second case involved surveillance only for limited time periods: Monday through Friday between 7:00 a.m. and 6:00 p.m. and Saturday from 7:00 a.m. to 1:00 p.m. Tr. of Proceedings at 299-300, *United States v. Caraballo*, No. 4:08-cr-35 (E.D. Va. Dec. 11, 2008), ECF No. 52, *aff'd* 384 F. App'x 285 (4th Cir. 2010). The government's other examples involved surveillance of one or more stationary locations—an exercise that is far less invasive and resource-intensive than tailing a suspect on the move. *See Young v. Owens*, 577 F. App'x 410, 412 (6th Cir. 2014) (store); *United States v. Gaskins*, 690 F.3d 569, 574 (D.C. Cir. 2012) (multiple locations) *United States v. Johnson*, 480 F. App'x 835, 837 (6th Cir. 2012) (residence); *Shades Ridge Holding Co. v. CIR*, 23 T.C.M. (CCH) 1665 (1964) (home).

In the end, the government's examples simply reinforce the concurring Justices' conclusion in *Jones* that it is extremely rare for law enforcement to tail a suspect for any significant period. *See Jones*, 565 U.S. at 430 (Alito, J., concurring in the judgment). And in this case, where police developed suspicion about petitioner only *after* the fact, and then sought to go back in time and recreate his past locations and movements over several months, the ability to gather location data has traditionally been even more constrained.

B. Procuring CSLI Intrudes on People's "Papers" Under the Fourth Amendment.

Neither of the government's responses to petitioner's property-based argument that a search occurred here withstands scrutiny.

1. Contrary to the government's assertion, Resp. Br. 41, petitioner's property-based argument is properly presented. The property-based rationale is an alternative argument supporting petitioner's legal claim that the government's acquisition of CSLI constitutes a search. "[O]nce a federal claim is properly presented, a party can make any argument in support of that claim; parties are not limited to the precise arguments they made below." *Lebron v. Nat'l R.R. Passenger Corp.*, 513 U.S. 374, 379 (1995). In any event, this Court may consider any argument that was "passed upon" by the court below. *United States v. Williams*, 504 U.S. 36, 41 (1992). The Sixth Circuit addressed this argument, holding that "[t]he

defendants of course lack any property interest in [the] cell-site records." Pet. App. 12a.[2]

2. On the merits, the government argues that the Telecommunications Act cannot create a proprietary interest in CSLI because it provides exceptions to its nondisclosure rule. Resp. Br. 42. But as petitioner has explained, the statute creates a property interest because it provides cell phone users with the rights to exclude others from their CSLI and to limit its use. Petr. Br. 33-34. That the service provider retains possession of, and a limited right to use, the records does not alter this conclusion. A person need not possess *all* of the "bundle of sticks" of property rights in order to have a protected interest in a location or thing. *See Dickman v. C.I.R.*, 465 U.S. 330, 336 (1984). That is why the Federal Communication Commission has concluded –in a determination the government never mentions, much less refutes –that papers containing CSLI are *customers'* records. Petr. Br. 33-34.

---

[2] The government also incorrectly asserts that the parties' joint stipulation that the CSLI records "are authentic and accurate business records of the[service providers]," JA 51, precludes petitioner's argument here. Resp. Br. 18, 41-42. That stipulation simply allowed the government to avoid calling employees of the companies to testify to their recordkeeping practices. *See* Fed. R. Evid. 803(6) (exception to hearsay rule for certain records kept by businesses). It was not a substantive determination about petitioner's privacy or property interest.

C. The Government's Theory Would Negate Fourth Amendment Protection For A Wide Range Of Vital Privacy Interests In The Digital Age.

Attempting to reassure the Court that its proposed rule won't sweep too far, the government suggests that the contents of electronic communications and other digital information might be exempted from the third-party doctrine. Resp. Br. 36-38. While the contents of emails and other digital-age communications are surely protected by the Fourth Amendment, the government provides an unconvincing account of how they can be distinguished from the records at issue here.

1. The government posits a distinction between information "communicated *to* the providers" and information that "merely passes *through* their communications networks, with no general right of the provider to use or control the contents." Resp. Br. 36-37. That may provide a clean distinction for physical letters, which remain sealed in transit, *see Ex Parte Jackson*, 96 U.S. 727, 733 (1877), but it fails to accurately reflect the way emails are handled.

In fact, service providers *do* retain the right to access the contents of emails. As the government has recently explained elsewhere, "the terms of service currently applicable to Microsoft's free email service do not suggest a mere caretaker or trust relationship. Rather, they assert Microsoft's right to access or use the *contents* of its customers' emails." Br. for the U.S., *Microsoft v. United States*, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2015 WL 1139654, at *41,

cert. granted, No. 17-2 (Oct. 16, 2017). Other major email service providers also access the contents of emails to provide "customized search results, tailored advertising, and spam and malware detection," among other purposes. Google Terms of Service, https://www.google.com/policies/terms; *see also* Final Reply Br. for Def.-Appellant U.S., *Warshak v. United States*, 532 F.3d 521 (6th Cir. 2008) (No. 06-4092), 2007 WL 2085416 ("Yahoo! has access to and control over the e-mail stored on its servers.").

Thus, if the content of email is protected by the Fourth Amendment, it is not because of how email is transmitted or exposed to service providers. Rather, it is because of the strong expectation of privacy in email notwithstanding providers' access. CSLI should be protected for the same reason. Just as people have never expected the government to have free access to the contents of their private communications merely because they are transmitted through third parties, they have never expected that the government would be able to obtain a pervasive record of their past locations and movements upon request.

2. Email is just the beginning. As the Technology Companies explain, "all digital technology transmits user information to various service providers[, and t]hose transmissions are an unavoidable condition of using digital technology." Tech. Cos. Br. 18. Much of this information is *provided to* rather than *transmitted through* third parties. Thus, under the government's theory, such information would be available to the government without any Fourth Amendment protections—including "health and fitness data" from a

smartphone app or smartwatch, information about "a homeowner's habits" from internet-of-things devices in the home, and the entire record of what a person searches, browses, or reads online. *Id.* at 18-19; Petr. Br. 44-47.

II. WARRANTLESS SEARCH OF LONGER-TERM HISTORICAL CSLI IS UNREASONABLE UNDER THE FOURTH AMENDMENT.

If this Court reaches the issue, it should hold that a warrant is required to conduct a search of CSLI. None of the government's arguments to the contrary has merit.

A. The Subpoena Power Does Not Allow The Government To Obtain Records Held By A Third Party In Which There Is A Reasonable Expectation Of Privacy.

The government does not contest that this Court's opinions upholding use of subpoenas to obtain records from third parties have never addressed a situation in which the subject of the investigation has a reasonable expectation of privacy or property interest in the records. The government attempts to explain this away by asserting that it "is because the Court applied the third-party doctrine" in those cases. Resp. Br. 47 n.12. But that is a perfectly circular explanation. If records in a third party's possession do implicate a subject's reasonable expectation of privacy, a subpoena is not sufficient to satisfy the Fourth Amendment.

First-party subpoenas generally satisfy the Fourth Amendment for two reasons: (1) they are less intrusive than a typical search, because the subject himself produces the material; and (2) they permit the subject to challenge the subpoena before his privacy is invaded. *See Donovan v. Lone Steer, Inc.*, 464 U.S. 408, 414-15 (1984); Resp. Br. 45. Neither rationale applies where, as here, a subpoena seeks information from a third party in which the subject has a reasonable expectation of privacy. In that context, (1) a subpoena is just as intrusive of the subject's privacy as any full-scale search of the third party would be; and (2) the subject has no pre-enforcement opportunity to challenge the subpoena, as he lacks notice.

None of the government's fallback arguments hold water either.

1. The government first (and most dramatically) seeks a categorical rule of form over substance, asking the Court to hold that once investigators have chosen to proceed via subpoena, that choice should be upheld without regard to the expectation of privacy in the information sought. Resp. Br. 47. Not surprisingly, that cannot be squared with this Court's analysis in third-party subpoena cases. In those cases, the Court has carefully assessed whether the subject of the investigation has a reasonable expectation of privacy in the records requested. *See, e.g.*, *Miller*, 425 U.S. at 442; *Couch v. United States*, 409 U.S. 332, 336 (1973); *see also Fisher v. United States*, 425 U.S. 391, 399, 401 n.6 (1976). The only coherent reason for doing so is that, where such expectation exists, it renders the subpoena unreasonable.

Indeed, the government's theory countenances *no* type of record or information for which criminal investigators would be required to seek a warrant: not the data from a suspect's phone stored in the cloud, *but see Riley*, 134 S. Ct. at 2491, or the contents of her emails held by a provider, *but see United States v. Warshak*, 631 F.3d 266, 285-88 (6th Cir. 2010).

It is no answer to say, as the government does, that "the subpoena standard itself" can "impose more stringent requirements depending on the nature of the requested documents." Resp. Br. 48. Under this approach, magistrates would have to decide when information poses "[s]pecial problems of privacy" and draw distinctions between "relevance" and "unquestionable relevance." *Id.* (alteration in original and citation omitted). It would be far clearer to enforce the familiar warrant requirement than to require magistrates to apply such novel and amorphous tools to manage governmental requests to conduct searches.

Moreover, the government misreads even the case on which it relies for its suggested enlargement of the subpoena power. *Id.* In *Fisher v. United States*, taxpayers and attorneys challenging summonses for tax preparation materials did not raise Fourth Amendment arguments. 425 U.S. at 401 n.7. In dicta, the Court noted that any such argument would fail because the request at issue *itself* sought "only documents of unquestionable relevance." *Id.* The Court then went on to explain that "[s]pecial problems of privacy which might be presented by subpoena of a personal diary are not involved here." *Id.* (citation omitted). The implication is that even an

"unquestionabl[y] relevant" subpoena could not compel production of something as private as a diary entrusted to the care of another.

2. The government next argues that requiring a warrant here "would impede longstanding investigatory practices" involving subpoenas. Resp. Br. 49. But requiring a warrant for CSLI will leave the government's compulsory process power intact in the vast majority of cases. A warrant requirement here will have no bearing, for example, on administrative subpoenas issued in regulatory investigations, where the special-needs exception applies. *See v. City of Seattle*, 387 U.S. 541, 544-45 (1967). It will likewise not impede use of criminal investigative subpoenas in the multitude of cases where the government seeks corporate books, tax records, or other documents in which courts have held that no person has a reasonable expectation of privacy. *See, e.g.*, *Couch*, 409 U.S. at 336 & n.19.

3. The government lastly maintains that the lack of notice that flows from using its subpoena power is acceptable because contemporaneous notice is not required for warrants either. But in the context of records held by third parties in which a reasonable expectation of privacy exists, the requirement of a warrant is a *substitute* for the right to pre-enforcement challenge that would otherwise accompany a first-party subpoena. Warrants, which issue upon probable cause, supported by oath or affirmation, and describe with particularity the scope of the search, provide critical procedural and substantive safeguards when the investigative target cannot advance her own rights.

The government responds that the service provider can object before producing records. Resp. Br. 45. But service providers will generally lack the incentive or knowledge to raise their subscribers' Fourth Amendment interests. And even when providers have done so in other cases, the government has argued that they lack such authority. *See* Mot. To Dismiss 10, *Microsoft v. U.S. Dep't of Justice*, 233 F. Supp. 3d 887 (W.D. Wash. 2017) (No. C16-0638), 2016 WL 4120319 (citing *Alderman v. United States*, 394 U.S. 165, 174 (1969)). In the absence of notice, only a warrant can safeguard the populace's Fourth Amendment rights.

B. Principles Of Fourth Amendment Reasonableness Require A Warrant.

As a last resort, the government invites this Court to assess the legitimacy of the search here through a general balancing of interests. Resp. Br. 50. But the only authority the government cites in this respect is *Maryland v. King*, in which this Court applied the "special needs" doctrine to uphold limited searches of a category of people—arrestees—with diminished expectations of privacy. 133 S. Ct. 1958, 1969-70, 1978 (2013). That *King* does not apply here is reason enough to reject the government's argument. *See* Petr. Br. 49. At any rate, a balancing of interests confirms that conducting a warrantless search of longer-term historical CSLI is unreasonable.

1. On one side of the balance, the privacy interest in not having the government know where one has traveled minute-by-minute over extended periods is high. And absent any constitutional check, Section 2703(d) does not prevent police from

obtaining huge swaths of CSLI—more than a year's worth in some cases—thus exposing large volumes of private information to government scrutiny. *See, e.g.*, *United States v. Brown*, 2017 WL 4216979, at *5 (D. Neb. 2017) (454, 388, and 186 days of suspects' CSLI). Only the probable cause and particularity requirements of a warrant can provide appropriate protection.

2. On the other side of the balance, the government lacks a sufficiently compelling interest to overcome the presumptive requirement of a warrant.

The government asserts an interest in accessing CSLI "during the early stages of an investigation, when the police [may] lack probable cause." Resp. Br. 51 (alteration in original). But that argument can be advanced about *every* search. In *Jones*, for example, the government asserted the same "interest of law enforcement in investigating leads and tips . . . before those suspicions have ripened into probable cause." U.S. Reply Br. 22, *Jones* (No. 10-1259). This Court rejected the argument and should do so again here. Under petitioner's rule, as under the concurring opinions in *Jones*, the government may obtain shorter-term locational information without a warrant. That generally satisfies any legitimate interest in collecting evidence early in an investigation, before the government has developed probable cause. *See* Resp. Br. 52 (citing cases where the government obtained, or could have obtained, short-term CSLI); State AGs Br. 20-22 (same).

Further, in the mine-run of cases, the government likely already has probable cause when it applies for a 2703(d) order, as demonstrated by the

facts set out in the applications in numerous cases. *See, e.g.*, *Ford v. State*, 477 S.W.3d 321, 325 (Tex. Crim. App. 2015) (finding that the application under § 2703(d) actually established probable cause). A warrant requirement will impose no undue burden.

C. Congressional Inaction Is Irrelevant Here.

Petitioner has already explained why the SCA does not represent "a judgment by Congress" as to how to appropriately protect historical CSLI, Resp. Br. 53. Congress did not contemplate the existence of historical CSLI, let alone its future ubiquity, when crafting the statute. Petr. Br. 49-50.

The government argues that Congress has since considered and declined to enact various amendments to the SCA that would have addressed CSLI more directly. Resp. Br. 54-55. But as this Court has repeatedly explained, "[c]ongressional inaction lacks persuasive significance because several equally tenable inferences may be drawn from such inaction." *Pension Ben. Guar. Corp. v. LTV Corp.*, 496 U.S. 633, 650 (1990) (internal quotation marks omitted). That is especially the case here, where legislative chokepoints have stymied overwhelmingly popular attempts to update the SCA. *See, e.g.*, Email Privacy Act, H.R. 699, 114th Cong. (2015) (passed by House on unanimous vote, but unable to receive vote in Senate).

Absent meaningful legislative action, the task once again falls on this Court to enforce the requirements of the Fourth Amendment. It should do so here to preserve the reasonable expectation of

privacy that Americans have long enjoyed in the details of their location over a long period.

CONCLUSION

For the foregoing reasons, the judgment of the Sixth Circuit should be reversed.

Respectfully submitted,

Nathan Freed Wessler
Ben Wizner
Brett Max Kaufman
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
New York, NY 10004

David D. Cole
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
915 15th Street, NW
Washington, D.C. 20005

Cecillia D. Wang
Jennifer Stisa Granick
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
39 Drumm Street
San Francisco, CA 94111

Harold Gurewitz
Counsel of Record
GUREWITZ & RABEN, PLC
333 W. Fort Street, Suite 1400
Detroit, MI 48226
(313) 628-4733
hgurewitz@grplc.com

Daniel S. Korobkin
Michael J. Steinberg
Kary L. Moss
AMERICAN CIVIL LIBERTIES UNION FUND OF MICHIGAN
2966 Woodward Ave.
Detroit, MI 48201

Jeffrey L. Fisher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305

Dated: October 24, 2017